REMARKS

The application has been amended and is believed to be in condition for allowance.

The indication that claims 3, 4, and 7-13 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims is acknowledged with thanks.

New claims 113-143 are introduced to further claim the invention, finding support in the specification and the figures and introducing no new matter.

The Official Action states that the information disclosure statement filed 11/19/03, and 10/07/05 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because there is no English translation.

In response, it is noted that the information disclosure statement filed 11/19/03 stated that a description of the relevance of the disclosed items is provided in pages 1-7 of the specification, the specification filed in English. As to the information disclosure statement filed 10/07/05, a concise description of the relevance of the disclosed items was provided with an English translation.

The undersigned confirms that the PAIR database shows that these references were received by the Patent and Trademark

Office. Consideration of these references and an initialed ITO form is respectfully requested.

The Official Action rejects claim 59 under 35 USC 112, second paragraph.

In response it is noted that claim 59 has been cancelled without prejudice.

The Official Action rejects claims 1, 2, 5, 6, and 59 under 35 USC 103(a) as being unpatentable over Lachman III US 2002/0166063 (hereinafter LACHMAN) in view of Sheymov US 7,010,698 (hereinafter SHEYMOV).

The Official Action states as to claims 1 and 59 that LACHMAN teaches an attack defending system wherein a filtering condition manager for managing the filtering condition depending on whether the attack detector detects an attack based on the input IP packet forwarded to the decoy device.

The Official Action acknowledges that LACHMAN does not disclose a decoy device that comprises an attack detector.

The Official Action states that SHEYMOV discloses an attack detector for detecting presence or absence of an attack by executing a service process for the input IP packet transferred from the firewall device

The Official Action concludes that it would have been obvious to one of ordinary skill in the art to use the attack detection decoy of SHEYMOV with the system of LACHMAN because it

removes the need for additional attack detection devices thus lowering cost.

In response, Applicant notes that claim 59 has been cancelled, as stated above. It is also noted that claim 1 has been amended to clarify the recitation. The amendment is non-substantive, and does not introduce new matter.

Applicant further notes that the Official Action does not identify with specificity any element in LACHMAN corresponding to either (1) the filtering condition manager or (2) a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet. Should this rejection not be withdrawn, Applicant respectfully requests identification of each element or passage in the cited reference believed to satisfy each claim recitation. It is respectfully submitted that this is necessary to afford the Applicant an opportunity to understand and respond to the rejection.

It is respectfully submitted that neither LACHMAN nor SHEYMOV, individually or in combination, disclose a firewall forwarding an IP packet wherein a destination selector selects, as an output destination of the firewall, a decoy device or any other device as a destination of the input IP packet based on the header information of the input IP packet and a distribution condition, as required by claim 1.

In contrast, when the LACHMAN system determines input packets to be malicious, the packets are merely blocked, LACHMAN paragraph 0109 (e.g. directed to a null route, LACHMAN paragraph 0115). Therefore, LACHMAN does not disclose any means or mechanism to forward an input IP packet to a decoy device or select the decoy device as an alternative destination.

It is also respectfully submitted that neither LACHMAN nor SHEYMOV, individually or in combination, disclose an attack detector receiving the input IP packet from the firewall device, and executing a network service process responsive to the input IP packet, as recited in claim 1. Neither reference teaches running a network service process. Further, there is no teaching in SHEYMOV of interaction with a firewall or any other network security device, and SHEYMOV does not teach any application to IP packets.

In contrast, SHEYMOV creates a "code inspection system," an accurate copy of a protected computer or device, for testing suspicious files (SHEYMOV, column 1, lines 38-40; column 2, lines 60-63). "The static test chamber system allows for the detection of malicious code that can be incorporated into files of applications, such as an e-mail or program, or that may be self-executing," column 2 lines 5-7.

In other words, the attack detector of SHEYMOV executes a code inspection module that in turn maintains a mirrored computer system that receives code, in the form of files or

applications, and subsequently executes and evaluates that code and its effect upon the mirror system.

SHEYMOV provides no teaching, either in the figures or the specification, of the code inspection system either receiving an input IP packet or executing a network service process responsive to the input IP packet, as required by claim 1.

As well known in the art, an input IP packet has no impact on a computer system unless a network service process, responsive to the input IP packet, is executed on the system. For example, a computer system receiving a Telnet packet through a network interface connected to a network will not respond (e.g., ignore the packet) unless a Telnet service process is run on that system (see specification of the instant invention, page 24, lines 6-7).

In other words, an input IP packet does not execute. On the contrary, code, as disclosed by SHEYMOV, may be introduced, executed, and even cleaned on the inspection system (e.g., SHEYMOV column 9, lines 1-21; SHEYMOV claim 2), despite there being no network service process disclosed as part of the SHEYMOV invention. Therefore, input IP packets as recited in claim 1 are neither described nor suggested by SHEYMOV's code.

In addition, SHEYMOV does not disclose, expressly or otherwise, receiving an input IP packet from a firewall device, as recited in claim 1. SHEYMOV only discloses that code to be tested is introduced (e.g., SHEYMOV column 9, lines 1-3); SHEYMOV

provides no disclosure how the code is introduced into the mirror system before it is executed or cleaned.

Accordingly, it is respectfully submitted that neither SHEYMOV nor LACHMAN, individually or in combination, disclose all the elements recited claim 1.

It is further submitted that the combination of references proposed in the Official Action would neither lead to the present invention nor be obvious to one skilled in the art.

SHEYMOV, as indicated above, does not disclose an attack detector executing a network service process responsive to input IP packets. Moreover, SHEYMOV does not disclose any network process service nor any subject matter relating to IP packets.

In other words, SHEYMOV does not disclose anything that would act or respond in a combination of LACHMAN and SHEYMOV where the firewall disclosed in LACHMAN would presumably be configured to transfer suspicious IP packets to it instead of to a null route. That is, SHEYMOV discloses no capability to detect the presence or absence of an attack in response to input IP packets, as recited in claim 1, and thus would not function to improve upon the capability of LACHMAN, removing a need for additional attack detection devices.

Therefore, it is respectfully submitted that one of skill would not combine these references, and the proposed combination would not produce an attack detection system as

claimed in claim 1. Accordingly, the proposed combination would not have been obvious to one skilled in the art.

For all the foregoing reasons, reconsideration and withdrawal of the 35 USC 103(a) rejection of claim 1 and claims depending therefrom are respectfully solicited.

In addition, new claims 113-142 combine the limitations of claim 1 as originally filed with the limitations of claims 3, 4, and 7-13, indicated as allowable if amended into independent form. Accordingly, it is believed these claims are patentable as presented.

New claim 143 is believed to be patentable for the same reasons stated above regarding claim 1.

From the foregoing, it will be apparent that applicants have fully responded to the July 27, 2007 Official Action and that the claims as presented are patentable. In view of this, applicants respectfully request reconsideration of the claims, as presented, and their early passage to issue.

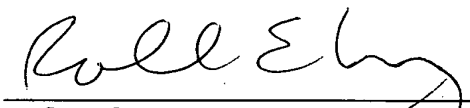
In order to expedite the prosecution of this case, it is requested that the Examiner telephone the attorney for applicants at the number set forth below if the Examiner is of the opinion that further discussion of this case would be helpful.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any

overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



Roland E. Long, Jr., Reg. No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

REL/jlw